Kary organów nadzorczych w Unii Europejskiej

Kraj oraz organ nadzorczy
Szwecja
Data Protection Authority of Sweden

Data wydania decyzji
26 kwietnia 2023

Podmiot kontrolowany
Skåne region

Wysokość kary
17 600 EUR

FORSAFE
BEZPIECZEŃSTWO PONAD WSZYSTKO

Rodzaj naruszenia

Art. 32 (1) RODO
Niewystarczające środki techniczne i organizacyjne zapewniające bezpieczeństwo informacji.

Przedmiot decyzji

Źródło postępowania:

W listopadzie 2020 r. do szwedzkiego organu nadzorczego wpłynęło zgłoszenie naruszenia ochrony danych osobowych od Skåne region polegające na zgubieniu zewnętrznego nośnika danych na skutek umieszczenia przez pracownika pendriva w kieszeni odzieży klinicznej, która została przekazana do prania.

Opis wydarzeń:

1. Skåne region w wysłanym zgłoszeniu poinformował, iż na pendrivie znajdowały się numery ubezpieczenia społecznego oraz dane o stanie zdrowia 1934 osób.

2. Szwedzki organ nadzorczy zdecydował o dokonaniu czynności kontrolnych w Skåne region celem rozpatrzenia przedmiotowej sprawy.

3. W trakcie czynności kontrolnych szwedzki organ nadzorczy ustalił, iż dane znajdujące się na pendrivie zostały przekazane pracownikowi Skåne region przez Uppsala Clinical Research Center w celach badawczych a wspomniany pracownik zobowiązał się do przechowywania danych w sposób bezpieczny oraz w postaci zaszyfrowanej.

4. Na podstawie zebranego materiału dowodowego szwedzki organ nadzorczy uznał, że Skåne region nie wdrożył odpowiednich środków technicznych i organizacyjnych zapewniających stopień bezpieczeństwa odpowiadający ryzyku przetwarzania danych przy użyciu zewnętrznych nośników danych.

Przyczyna naruszenia:

Pracownik Skåne region zgubił zewnętrzny nośnik danych zawierający dane osobowe.

Decyzja:

Kara pieniężna w wysokości 200 000 SEK (17 600 EUR).

Źródło:

https://www.imy.se/globalassets/dokument/beslut/2023/beslut-tillsyn-region-skane.pdf

Kompas FORSAFE

JAK UNIKAĆ TAKICH NARUSZEŃ?

1. Dokonując wyboru odpowiednich środków technicznych i organizacyjnych pamiętaj, że jest to proces dwuetapowy. W pierwszej kolejności ważne jest, aby określić poziom ryzyka, jaki wiąże się z przetwarzaniem danych osobowych. Dopiero po wykonaniu tej czynności możemy ustalić, jakie środki techniczne i organizacyjne będą odpowiednie, aby zapewnić stopień bezpieczeństwa odpowiadający temu ryzyku.

2. Dokonuj regularnego testowania, mierzenia i oceniania skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania danych osobowych w systemach teleinformatycznych.

Materiał edukacyjny przygotowany przez FORSAFE

Opracowanie merytoryczne
Katarzyna Kawczyńska